PRIVATE BRANCH EXCHANGE (PBX)

PROTECTION PROFILE

National Institute for Standards and Technology

Foreword

This publication, Private Branch Exchange (PBX) Protection Profile, is issued by the National Institute of Standards and Technology (NIST) as part of its program to promulgate security standards for information systems. This protection profile was developed through the efforts of Dr. Ron Bhattacharyya of Telcordia Technologies Inc., Jandria S. Alexander, Edward J. Coyne and Robert L. Williamson, Jr, or SAIC and Donald G. Marks of NIST.

Comments on this document should be directed to:

Dr. Donald G. Marks
NIST/Computer Security Division
100 Bureau Dr., Stop 8930
Gaithersburg, MD. 20899-8930

(301) 975-5342
donald.marks@nist.gov

TABLE OF CONTENTS

1. Introduction

1.1 Identification

Title: Private Branch Exchange Protection Profile (PBXPP)

Registration: National Institute of Standards and Technology

Keywords: Telecommunications, Switch, PBX, Information Security

1.2 Overview

The purpose of this document is to develop a Protection Profile (PP) using the Common Criteria (CC) for baseline PBX security that is believed to be achievable by deploying currently available Information Technology (IT). Care has been taken to formulate the PP in such a way as to provide a basis for future development of specific Security Targets (ST). It is expected that this PP could be used to develop a uniform test procedure suitable for implementation by appropriate third parties to test the level of security of a wide class of PBXs. The PP and the ensuing test procedure are intended to be internationally recognized, and endorsed by the industry trade associations. This will provide telecommunications customers with an independent evaluation of security features of their respective PBXs. The acceptance of these results will improve the security of the entire telecommunications network and allow more open competition among the various PBX manufacturers.

A Private Branch Exchange (PBX) is Customer Premises Equipment (CPE). A telecommunications service provider does not deploy a PBX to provide telecommunications service. Instead, a PBX belongs to a *customer* that subscribes to a telecommunications service, and is located in or about the premises/facilities of the said customer. In a typical PBX installation, adjuncts, such as a voice mail system and an automated attendant are logically connected to the PBX. The safe and secure upkeep of the PBX and its adjuncts is the responsibility of the owner, i.e., the customer of the telecommunications service.

If the PBX and its adjuncts are not adequately protected, they can be exploited by interlopers to make fraudulent phone calls and to commit other kinds of security breeches. A PBX owner is responsible for paying the telephone bills for calls placed from that PBX, whether the calls are genuine or not. To avoid having to pay for fraudulent bills, it is important that a PBX owner secures the PBX and its adjuncts against unauthorized use and modification/destruction of the embedded processes, software and database.

With the rapid advancement of digital technology, PBX systems have evolved from hard-wired, mechanical devices to flexible, dynamic, software-configurable devices. In effect, they have become specialized computers. Access to the PBX is no longer only provided from local connections. Remote access for maintenance and configuration management may be accomplished via remote access. This remote access has made PBX systems vulnerable to intrusion. The introduction of digitized voice has opened the PBX to Local Area Network (LAN) based data traffic, and hence, has introduced vulnerabilities inherent in a distributed architecture with multiple access

points. In addition, the trend towards "voice over IP" is creating new opportunities for using integrated voice and data networks for business-critical applications. However, these integrated networks, if not adequately protected, may have serious vulnerabilities of their own. The recent acceptance of the QSIG protocol as the communications standard among networked PBXs makes it possible to establish network connectivity among several PBXs manufactured by different vendors, and in turn exacerbates the risk to the PBX. As a result of these developments, PBX security has become a critical issue. Indeed, the PBX is an essential element that supports a "critical infrastructure" of the business community of the country, and protection of the PBX is a high priority.

1.3 Conventions

This document is organized based on Annex B of Part 1 of the Common Criteria (CC).

Application notes represent guidance and explanations of acceptable implementations for requirements. For additional guidance, the CC itself should be consulted.

1.4 Terms

The following terms, used in this profile, are described in this section to aid in the application of the requirements.

- TOE Security Function (TSF) – This is the hardware-software capability of performing security related functions for the protection of the TOE. Depending on the application, this capability does not need to be confined within the switch. For example, in a networked environment, the required security features can be deployed anywhere in the environment as long as they provide the intended security to the TOE. The functional requirements described in this PP are to be levied on the TSF.
- Target of Evaluation (TOE) – This is the entity the security of which is being addressed in this Protection Profile (PP). In the case of a PBX, which constitutes the target, the TOE consists of that PBX. However, if a PBX is protected by a peripheral security server, the target of security is not just the PBX but the total system consisting of the PBX and the peripheral security server.
- Adjunct - This is a peripheral device, external to the PBX, but logically connected to it, and supplements the functionality of the PBX by providing additional features. Examples are automated attendant, voice mail system, etc.
- Authorized Administrator - An authorized administrator is a user who performs administrative tasks such as creating, retrieving, updating and deleting security parameters (e.g., passwords, permission levels, etc.) in the PBX database. As such, the administrator has to be a highly privileged user of the PBX. Depending on the organization, the authorized administrator may have titles such as Security Administrator, System Administrator, etc.
- Customer - A customer is a person or organization that is a subscriber to a service offered by a telecommunications service provider. The PBX is a Customer Premises Equipment (CPE).

- Port - A port represents a point of interface with the PBX. Typically, these ports are attached to the PBX console. Two kinds of ports have been invoked in the PP: (i) the operations port and (ii) the signaling port. Operations ports allow access to the PBX to perform operations functions such as provisioning, maintenance, testing, etc. Signaling ports allow communications devices to be directly attached to the PBX.
- Resource - Broadly speaking, there are two types of resources, namely, hardware resources and software resources associated with a PBX. In this PP, the primary focus is on software resources embedded in the PBX. Examples are: the operating system, subsystems, software packages, databases, processes, etc.
- Resource Access - Resources are accessed by transmitting messages to the PBX to impact the software resources of the PBX. Examples include loading a patch, creating, modifying and deleting data, retrieving status reports, initiating a process, etc.
- Subscriber – A subscriber is one who accesses the PBX via its line interface to place and receive telephone calls (and data communication, if relevant). Typically, a subscriber belongs to the organization of the customer that owns the PBX.
- System Access - The system is accessed by establishing an operations session (i.e., login) with the PBX. In order to maintain security of the PBX, system access must be successfully completed before resource access is permitted.
- Users - The word “user” is not synonymous with the word “customer” or the word “subscriber”. While a customer is a purchaser of telecommunications service, and a subscriber is one that places and receives calls (typically in the customer’s organization), a user is one that is authorized to establish a session at an operations port of the PBX. Typical users of a PBX consist of crafts-persons, administrators, or machines that establish operations related sessions with the PBX. As such, a user could be a person or a machine/system. A valid user must have a user-ID by which the PBX recognizes the user.
- Intruder - An intruder is not authorized to establish a session with the PBX, and as such, is not a user even though the intrusion may be successful.
- Subject – The owner of a process executing on the PBX. Could be a user, customer, subscriber, or intruder.

2 TOE Description

The PP defines a set of security requirements to be levied on a Target of Evaluation (TOE). A TOE consists of the PBX, any adjunct equipment and the software and firmware of the system. A TOE is therefore a *PBX system,* rather than simply a PBX. A TOE evaluation is concerned with ensuring that a defined TOE Security Policy (TSP) is enforced over the TOE resources. Those portions of the TOE that must be relied on for the correct enforcement of the TSP are collectively referred to as the TOE Security Functions (TSF). The TSF consists of all hardware, software, and firmware of a TOE that is either directly or indirectly relied upon for security enforcement. Any part of the TOE, that is not part of the TSF, may fail or error in any way without violating the TSP. A TOE evaluation is a formal process of analysis and testing to ensure that the defined TOE Security Policy is enforced over the TOE resources.

This PP lists requirements that apply specifically to a PBX. A PBX is not a general- purpose computer, although it may share some characteristics and features of a computer. Essentially, it is a switch that is connected to a telephone company's switch via incoming and outgoing trunks (or lines). These trunks (lines) branch into multiple extensions as per that customer's specifications. These extensions are used by subscribers in the customer’s organization to place and receive calls. The PBX has embedded software containing specifiable data and translations, which ought to be customized and maintained by the customer (i.e., the PBX owner) to satisfy individual needs. For example, it is possible to specify which extension(s) may or may not receive direct calls from the outside. Similarly, the "Toll Diversion" feature makes it is possible to specify which extension may have what level of permission to place calls, e.g., intercom only, local, long distance, international, etc. These customizations are made by setting appropriate parameters in the PBX software.

Occasionally, two other peripherals are deployed as "adjuncts" to the PBX. One is the "Automated Attendant", and the other is "Voice Mail". An automated attendant is a customer premises equipment which automates the functions of a human receptionist. If an incoming call to an extension of the PBX is not answered, or if that extension is busy, the voice mail system can play a recorded message to the caller, and record an incoming message that the caller wishes to leave.

To secure a PBX system, one should ensure that the security functions described in the PP are satisfied by the PBX and its adjuncts.

A PBX has two kinds of ports: signal ports and operations ports. The signal ports support the communications traffic. In other words, wires, cables, trunks, etc., that are connected to these ports carry the communications traffic. The operations ports allow ingress into the embedded software of the PBX. Crafts-persons and administrators access the operations ports to perform operations functions such as provisioning, maintenance, testing, etc.

In order to protect PBX resources and maintain the quality of service, it is necessary to protect the operations ports from unauthorized use. In addition, the signal ports need to be protected against commission of fraud.

Crafts-persons authorized to perform operations on the PBX may belong to different categories depending on the operations functions performed by them and their level of expertise. This function is filled by the use of different *roles*, as specified in the Common Criteria. Different roles need to have different levels of access to the PBX. For example, the maintenance crew does not need access to provisioning commands. In addition, within the maintenance crew a less experienced crafts-person may have only the “read” permission, while an experienced one may be trusted with writing as well as reading. It is even possible for a single person to be authorized different roles. For example, a person who is normally a system administrator may also be authorized to act in the role of a maintenance person on occasion. Supervisors may be authorized to act in any of the roles filled by people they supervise.

3 Security Environment

3.1 Threats

Threats relate to the chance of a security breech that may lead to events such as disclosure of confidential information, commission of fraud, or service deterioration due to misuse, modification or destruction of physical and/or Information Technology (IT) resources. Thus the threats that a PBX may be subjected to have several dimensionalities. Threats might be caused by outsiders (e.g., intruders) or by insiders (e.g., employees of the service provider). Insider threats are not always a reflection of malice on the part of the employee as they may also be the result of inadvertent employee actions. In order to mitigate these threats, one needs to protect the PBX by implementing appropriate security measures.

Examples of threats are listed below.

- Physical threat - Physical damage to a PBX may be caused by natural causes such as fire, flood, earthquake, or by human action such as sabotage. This PP assumes that PBXs are installed in a physically secure environment. Hence physical security is not addressed here as an issue.
- Fraud - In the context of telecommunications, fraud implies successfully completing a call (voice or data) without paying the legitimate bill for the call. This can be done in several ways if proper precautions are not taken. Examples of fraud include:
  - DISA Misuse - A PBX may be equipped with a feature called the Direct Inward System Access (DISA)[1] which allows a subscriber to call the PBX from outside the PBX system, and then obtain a dial tone to place a call to a directory number outside the system. This feature allows a subscriber (such as, a traveling employee of a company) to call the company PBX from outside (i.e., via the trunk interface), and then use the company's telephone service to place calls, which may be economical compared to using a credit card to place long distance calls. However, if this access is not protected, an intruder may place calls at the expense of the PBX owner.
  - Misuse of Voice Mail - If the voice mail is configured such that an outside caller is allowed a second dial tone (e.g., by dialing zero after the recorded message is played), an intruder may misuse this facility to place fraudulent calls after receiving the second dial tone.
  - Black Box Fraud - Black Box fraud is committed when a Customer Premises Equipment (CPE) is "altered" (i.e., tampered with) in such a way that it becomes possible to place a call to that CPE and successfully complete that call without the caller being billed. Thus, if a fraudulent owner of a PBX deactivates the "Answer Supervision" feature of that PBX, it may be possible to place (and successfully complete) a "free call" to the PBX from a remote location (i.e., no bill is generated for the call). In order for the free call to be successful, it is also necessary that the telecommunications switch at the remote location allow

[1] DISA is an optional feature. Hence, in any given application, if DISA is not needed, it may not be deployed.

voice transmission[2] in spite of the fact that it (the remote switch) never received the Answer Supervision message from the PBX.

- Misuse of Attendant - If an Automated Attendant is configured in such a way as to provide a second dial tone without adequate verification of the caller, fraudulent calls can be placed after receiving the second dial tone.
- Cloning Wireless Telephone[3] - This applies in the case of a PBX that allows wireless extensions to its subscribers. A wireless phone has several "identifiers" (i.e., attributes by which one phone can be distinguished from another), out of which two are most commonly used for identification purposes. They are the Mobile Identification Number (MIN) and Electronic Serial Number (ESN). It may be possible for an interloper to find out the MIN and ESN of a legitimate subscriber. For example, the interloper may use a radio receiver to eavesdrop when the legitimate subscriber establishes a call, and pick up the corresponding MIN and ESN. Alternatively, the interloper may break into the database that contains the MINs and ESNs of a number of legitimate subscribers. With the knowledge of the MIN and ESN of a legitimate subscriber, the interloper may program them into a cloned phone and use the cloned phone to place calls. The PBX owner will be billed for these calls.

- Denial of Service – Attacks exploiting vulnerabilities in the protocols may lead to deterioration or even denial of service or functionality of the PBX. For example: if unauthorized access can be established to any branch of the communication channel (such as a CCS link or a TCP/IP link), it may be possible to flood the link with bogus messages causing severe deterioration (possibly denial) of service.
- Access Misuse – Misuse may occur either from legitimate users (i.e. insiders) or intruders. An authenticated user may perform an incorrect operations function (e.g., by mistake or out of malice) and may cause unauthorized modification, destruction, deletion, or disclosure of the PBX software and data. This threat may be caused by several factors including the possibility that the level of access permission granted to the user is higher than what the user needs to remain functional.
- Intrusion - An intruder may spoof as a legitimate user and break into an operations port of the PBX. At this point the intruder may misuse the permission level of the legitimate user and perform damaging operations functions such as:
    a) Modifying call restriction features of subscribers (e.g., only local calls, long distance calls, international calls, etc.)
    b) disclosing confidential data
    c) causing service deterioration by modifying the PBX software
    d) crashing the PBX

[2] There are switches that do not allow voice transmission without first receiving the answer supervision message from the called party, thus eliminating the chance of this kind of fraud. But several major switches do not provide this protective feature. Besides, for Advanced Intelligent Network (AIN) applications, this protection may not be implementable.

3 The threat of fraud by cloning has been mitigated by the introduction of new technology such as "RF Fingerprinting", and "Authentication via Secret Key Exchange (e.g., by using the CAVE algorithm)." These allow enhanced validation (beyond MIN and ESN confirmation) of a legitimate customer against an interloper, and disallow fraudulent calls.

e) removing all traces of intrusion (e.g., modifying the security log) so that it may not be readily detected

- Voice Mail Intrusion - If an intruder is able to crack the PIN number of a valid subscriber, the mailbox may be taken over by that intruder. This allows the intruder to perform activities such as listening to messages, and using the mailbox as a bulletin board.

- Insecure State Transition - At certain times the PBX may be vulnerable due to the fact that it is not in a secure state. For example:
  - After a system restart, the old security features may have washed out, and new features may not have been activated. (For example, all old passwords have reverted to the default system-password, and new passwords have not been assigned.)
  - The same may happen at the time of a disaster recovery.
  - At the time of installation the PBX may be vulnerable until the time that the default security features are customized.
- Insecure Security System - The security system itself provides the capabilities for system abuse and misuse. That is, compromise of the security system not only allows system abuse but also allows the elimination of all traceability and the insertion of trapdoors for later intrusions. For this reason, the security system must be carefully protected.
  - Illegally assigning free lines - This requires entering the operations database of a PBX and the voice mail to perform illegal provisioning.

3.2 Organizational Security Policies

Organizational security policies (denoted as P.xxx) are normally directed at individual users. However, the binding between users and executable programs is sometimes tenuous, so the term "subject" will be used to describe computer programs or processes when necessary to distinguish them from the actual person initiating the process. Security-related organizational policies include the following:

- P.Access - Access rights to specific data objects are determined by object attributes assigned to that object, subject identity, subject attributes, and environmental conditions as defined by the security policy. A service that a subject is not authorized for shall be denied to that subject.
- P.Availability - There shall be no denial of authorized service. A PBX access that a user is authorized for shall not be denied to that user. A service that a subscriber is authorized for shall not be denied to that subscriber.
- P.Administration - The authorized systems administrator shall properly activate, implement and maintain the security features associated with the TSF.
- P.Resiliency - If a security compromise occurs, the PBX shall continue to provide those services unaffected by that compromise.
- P.TMN Standards - The tasks related to "Prevention", "Detection", "Containment and Recovery", and "Security Administration" (as defined under TMN standards) shall be recognized and delegated to appropriate authorities. Prevention implies physical security, legal re-

view, risk analysis, and logical controls. Detection is associated with alarms, cameras, usage pattern analysis, revenue pattern analysis, security audit, investigation of security breech, etc. Containment and recovery, as the name implies, includes intrusion recovery, disaster recovery, legal action, apprehension, etc. Security administration involves the day to day activities of ensuring that protective features are activated, the security parameters are kept up to date, and the security weaknesses are corrected.

- P.Confidentiality - Confidential information shall not be made available to unauthorized entities (persons, machines, etc.).
- P.Usage – PBXs shall be used only for authorized purposes.
- P.Traceability - The PBX shall implement features (e.g., alarms, audit trails, etc.) to: (i) alert an administrator of a suspected security breech, and (ii) record security events in a log file so that in case a breech is suspected, an audit trail could be established as part of investigation, and (iii) record adequate audit detail to uniquely identify subjects, ports, and security relevant activities.
- P.Accountability - Each user in the organization shall be held accountable for PBX-related actions performed by that user.

3.3 Security Usage Assumptions

This section describes the security aspects of the environment in which the TOE will be, or is intended to be used. This includes information about the physical, personnel, and connectivity aspects of the environment.

3.3.1 Physical Assumptions

It is assumed that the resources of the TOE, except possibly the remote access facilities, will be installed in a physically secure environment which will be “reasonably safe” from typical natural hazards as well as from unauthorized physical access. An example of a “reasonably safe” system implies the following, as a minimum:

- A.Natural. The TOE shall be protected from environmental hazards.
  - A TOE shall be housed in a facility that shall conform to established local building standards, i.e., codes related to precautions against hazards due to fire, flood, earthquake, and inclement weather conditions such as tornado, hurricane, typhoon, etc. This includes, among other construction codes, appropriate installation of various types of alarms and an administrative mechanism to promptly respond to such alarms when activated.
- A.Environment. The TOE shall be adequately protected from intruders obtaining physical access to the PBX or related equipment, by means such as:
  - Lighting within and around a facility shall provide adequate visibility for security guards and cameras.
  - Entry into a facility from outside shall be restricted by means of electronic locks or trained guards & ID cards.

- All doors for entering the premises shall be alarmed during hours that are outside the normal business hours. All “exit only” doors (especially emergency exits) shall be alarmed all the time.
- All facility access points, parking lots or other designated areas shall be equipped with 24-hour camera monitoring.
- Terminals used for local access shall have the same level of physical security as that of the PBX.

- A.PhysicalAuthorization. Physical access to the TOE shall be controlled and restricted to those needing such access, through such means as:
  - All persons (i.e., employees, contractors, authorized visitors, etc.) in a TOE facility shall be issued appropriate company-designated badges that authorize the holders to specific facilities or areas which they need to access.
  - Within a given TOE facility, areas which are considered critical/sensitive shall have doors protected with electronic locks that allow entry only to authorized personnel, based on need to access. These doors shall be spring-loaded so that they will automatically close after they have been opened.
  - All visitors to a TOE facility shall sign and date a visitor log, shall be issued a visitor badge and, if necessary, be escorted. The log shall, as a minimum, record the visitor’s name, the name of the establishment he/she represents, citizenship, the TOE point of contact, purpose of visit, date and times of arrival and departure.
  - All visitor badges shall be date and time limited.

3.3.2 Personnel Assumptions

It is assumed that the following personnel conditions will exist:

- A.Expertise. Responsible individuals shall be available to perform the tasks associated with Prevention, Detection, Containment & Recovery, and Security Administration, as described in Section 3.2.
  - Security administrators shall be available to perform security analysis (i.e., testing the security features for conformance and nonconformance with PP) for new PBXs, new adjuncts, and new generics before they are installed.
- A.Clearance. Each TOE owner will have a formal process to be completed before a person may be deemed “responsible”. This process may include interviews, checking references, or an extensive background check.
- A.Training. Authorized users of the system shall be adequately trained. Individuals deemed critical for secure operation shall receive training in security awareness enabling them to
  a) effectively implement organizational security policies with respect to their discretionary actions and
  b) support the non-discretionary controls implemented to enforce these policies.

- A.Audit. Internal auditors as well as external auditors shall be available to conduct periodic security audits (reviews).
- A.Regress. Each TOE owner will have regress available to hold users accountable for their actions. Such regress may be either legal or administrative actions.

3.3.3 Connectivity Assumptions

PBXs are occasionally connected to a network containing many other devices. The overriding security principle in such a networked environment is that there can be no assumptions made about the security features of these other devices or the network itself. That is, everything is assumed to be insecure unless known otherwise. Specifically, it is assumed that the following connectivity assumptions exist:

- A.Ingress. It is assumed that there are three types of ingress into the operations ports of a PBX, namely, local access, remote dial-up access, and remote networked access.
  - There may be users who are authorized to access the PBX from terminals situated at remote locations, and they may use dial-up access or networked access to the PBX.
- A.Protocols. Networked accesses may use a wide range of protocols such as X.25, TCP/IP, CMIP, SNMP, and several proprietary protocols.
- A.InsecureRemote. Remote locations shall not be assumed to be secure.
- A.InsecureNetwork. Depending on the network connectivity, the network may or may not be secure.
- A.Hardware. The PBX hardware shall support the required functions.

4 Security Objectives

This section defines the security objectives of the TOE (denoted O.xxx) and its supporting environment. Security objectives, categorized as either Technical security objectives or non-Technical security objectives, reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified. All of the identified threats and organizational policies that are addressed by this PP can be found under one or more of the categories below.

4.1 Technical Security Objectives

- **O.DOMAIN SEPARATION:** The TSF shall create and maintain a separate domain or domains of execution in which it can execute without interference from all subjects outside of this domain.
- **O.KNOWN**: The TOE shall ensure that, except for a well-defined set of allowed actions, all users are identified and authenticated before being granted access to the TOE or its resources.
- **O.ACCESS**: The TOE shall allow access by authenticated users to those TOE resources for which they have been authorized, and deny access to those TOE resources for which they are not authorized.
- **O.MISUSE**: The TSF shall mitigate the threat of malicious actions by authenticated users (e.g. by holding all authenticated users accountable).
- **O.AUTHORIZE**: The TOE shall provide the ability to specify and manage “resource access permission” to be assigned to its users.
- **O.BYPASS**: The TOE shall prevent all software and users from bypassing or circumventing TOE security policy enforcement.
- **O.ACCOUNT**: The TOE shall ensure that all TOE users can be held accountable for their security-relevant actions.
- **O.INFO-FLOW**: The TOE shall ensure that any information flow control policies are enforced - (1) between TOE components and (2) at the TOE external interfaces.
- **O.OBSERVE**: The TOE shall ensure that its security status is not misrepresented to the administrator or user.
- **O.DETECT**: The TOE shall have the capability to detect system failure and breech of security.
- **O.RECOVER**: The TOE shall provide for recovery to a secure state following a system failure, discontinuity of service, or detection of a security flaw or breech.
- **O.AVAILABLE**: The TOE shall protect itself from denial-of-service attacks, including those due to shared resource exhaustion.
- **O.NETWORK**: The TOE shall have the capability to meet its security objectives in a networked environment.

- **O.CONFIDENTIAL**: The TOE shall have the ability to identify confidential information. Such information may be related to customers, subscribers, or system security. The TOE shall release confidential information only to authorized users.

4.2 Non-Technical Security Objectives

- **O.PHYSICAL**: An administrator responsible for TOE security shall ensure that the TOE environment has adequate physical security to provide "reasonable safety" (as described earlier) to TOE resources.
- **O.OPERATE**: An administrator responsible for TOE security shall ensure that the TOE is delivered, installed, and operated in a manner which maintains IT security.
- **O.MANAGE**: An administrator responsible for TOE security shall ensure that the TOE is managed and administered in a manner that maintains IT security.
- **O.COMPLY**: The TOE environment shall support full compliance with laws, regulations, and contractual agreements.

4.3 General Assurance

It is desirable that applications, which require several distributed PBX installations interconnected with one another, shall provide layered security administration, in compliance with TMN standards. These standards specify five layers defined as:

a) Business Management Layer (BML) - which will be responsible for tasks such as Security policy, Disaster recovery plan, Assessment of data integrity, etc.
b) Service Management Layer (SML) - which will perform functions such as Administration of certification, Administration of security protocols, Customer audit trail management, and Customer security alarm management.
c) Network Management Layer (NML) - which will perform administration of security parameters at the overall network level.
d) Element Management Layer (EML) - which will perform administration of security parameters of a group of similar PBXs.
e) Network Element Layer (NEL) - which will provide local access at the PBX console.

It follows from the above definitions, that while BML and SML take care of the business and service related concerns associated with security, the three lower layers, namely, NML, EML, and NEL perform the PBX operations in a hierarchical way. Hence it is assumed that, as a minimum, these three layers will provide the required connectivity for distributed PBX operations.

TOEs compliant with this PP are targeted for near-term achievable, cost-effective, Commercial Off-The-Shelf (COTS) security. In keeping with this target, the general level of assurance for TOEs must:

- Be consistent with current best commercial practice for Telecommunications development and
- Enable evaluated products that are competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

TOEs compliant with this PP must meet an appropriate formal assurance level in order to be consistent with current and near-term mutual recognition agreements. This requires that the assurances:

- Be expressed as an existing evaluation assurance level (EAL) from part 3 of the Common Criteria; augmented by CC assurance components as required
- Contain no assurance components first appearing in EAL5 or above

Although most computer security products only meet level EAL2, the telecommunications industry is, in general, concerned with reliability, security, and good software engineering techniques. This care in the software development and design provides a higher assurance level for telecommunications switches than for most commercial computer software products. Therefore, EAL3 was selected as a reasonable target for this PP.

5 Functional Requirements

The policies, assumptions, and objectives generally define high-level descriptions of desirable security features. These high-level statements are implemented by combinations of low-level, specific functions. This chapter defines the functional requirements for the TOE. Functional requirements components in this profile were drawn from Part 2 of the CC.

CC defined operations for assignment, selection, and refinement are used to tailor the requirements to the level of detail necessary to meet the stated security objectives. These operations are indicated by lists enclosed in brackets [ ] for assignments and selections, and italicized text for refinements. Assignments and selections should be performed upon instantiation of the PP into a Security Target (ST) specification.

5.1 Protection of the TOE Security Functions (FPT)

5.1.1 Abstract Machine Testing (FPT_AMT.1)

The TOE Security Functions will depend upon the proper functioning of the underlying hardware and primitive operating system functions such as device drivers, protocol handlers, or hardware page protection. This underlying hardware/software platform will vary by manufacturer, but the *abstract* functions will be identical. The combination is therefore referred to as an *abstract machine*, and must be periodically tested for correct operation although its functions are not covered by the Protection Profile.

5.1.1.1 FPT_AMT.1.1. The TSF shall run a suite of tests [selection: *during initial start-up, periodically during normal operation, at the request of an authorized administrator, other conditions*] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

5.1.2 Fail Secure (FPT_FLS.1)

5.1.2.1 FPT_FLS.1.1. The TSF shall preserve a secure state when the following types of failures occur: [assignment:

a) *Audit log overflow.*
b) *Failure of individual channels or ports.*
c) *Failure of trunk.*
d) *Failure of lines.*]

5.1.3 Inter-TSF trusted channel (FPT_ITC.1)

5.1.3.1 FTP_ITC.1.1. The TSF shall protect sensitive TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

5.1.4 Inter-TSF detection and correction of modification (FPT_ITI.2)

5.1.4.1 FPT_ITI.2.1. The TSF shall provide the capability to detect modification of sensitive TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [assignment: *a defined modification metric*].

5.1.4.2 FPT_ITI.2.2. The TSF shall provide the capability to verify the integrity of sensitive TSF data transmitted to the TSF from a remote trusted IT product and perform [assignment: *action to be taken*] if modifications are detected.

5.1.5 Automated Recovery (FPT_RCV.2)

5.1.5.1 FPT_RCV.2.2. For [assignment: *list of failures/service discontinuities*], the TSF shall ensure the return of the TOE to a secure state using automated procedures.

5.1.5.2 FPT_RCV.2.1 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

5.1.6 Reference Mediation (FPT_RVM.1)

The requirements of this family address the “always invoked” aspect of a traditional reference monitor. The goal of this family is to ensure, with respect to a given TSP, that all actions requiring policy enforcement are validated by the TSF.

5.1.6.1 FPT_RVM.1.1. The TSF shall ensure that the TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.7 Domain Separation (FPT_SEP.1)

The components of this family ensure that at least one security domain is available for the TSF’s own execution and that the TSF is protected from external interference and tampering (e.g. by modification of the TSF code or data structures) by untrusted subjects.

5.1.7.1 FPT_SEP.1.1. The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

5.1.7.2 FPT_SEP.1.2. The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.8 Simple trusted acknowledgement (FPT_SSP.1)

5.1.8.1 FPT_SSP.1.1. The TSF shall acknowledge, when requested by another part of the TSF, the receipt of unmodified TSF data transmission.

5.1.9 Reliable Time Stamps (FPT_STM.1)

5.1.9.1 FPT_STM.1.1. The TSF shall be able to provide reliable time stamps for its own use.

5.2 Identification and Authentication (FIA)

5.2.1 Authentication Failure Handling (FIA_AFL.1)

5.2.1.1 FIA_AFL.1.1. The TSF shall detect when [assignment: number] of unsuccessful authentication attempts occur related to consecutive login failures, or consecutive DISA access failures.

5.2.1.2 FIA_AFL.1.2. When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment:

- *lock the channel for the amount of time set by the authorized administrator, and send a notification to the authorized administrator, or*
- *other authorized action*]

a) If DISA is deployed on the PBX, when the defined number of unsuccessful DISA authentication attempts has been met or surpassed, the TSF shall [assignment:
   - *lock the DISA entry for the amount of time set by the authorized administrator, and generate an alarm or send a notification to the authorized administrator, or*
   - *other authorized action]*

b) If Voice Mail is deployed on the PBX, when the defined number of unsuccessful Mailbox-PIN authentication attempts has been met or surpassed, the TSF shall [assignment:
   - *lock the mailbox for the amount of time set by the authorized administrator, and/or generate an alarm or send a notification to the authorized administrator or*
   - *other authorized action]*

5.2.2 User Attribute Definition (FIA_ATD.1)

5.2.2.1 FIA_ATD.1.1. The TSF shall maintain the following list of security attributes belonging to individual users: [assignment:

a) *User Identifier;*
b) *Roles;*
c) *Authentication Data, such as passwords;*
d) *Port and Channel permissions;*
e) *ST writer specified user security attributes;*
f) *If DISA is deployed on the PBX*
g) *The DISA Directory Number*
h) *The DISA PIN number for DISA subscribers*
i) *The DISA authorization codes ;*
j) *Other security attributes*]

5.2.2.2 FIA_ATD.1.2. The TSF shall maintain the following security attributes only in encrypted form [assignment:

a) *User passwords*
b) *Other selected user attributes as designated by the security administrator*
c) *DISA PIN numbers, if DISA is deployed*]

5.2.3 Strength of Authentication Data (FIA_SOS.1)

5.2.3.1 FIA_SOS.1.1. The TSF shall provide a mechanism to verify that secrets (i.e. data only available to the TSF) meet [assignment: *a quality metric defined by the authorized administrator*].

For example:
a) passwords may be required to be 8 characters long and contain at least one number;
b) DISA PIN numbers may be required to be 10 characters long;
c) Voice mail PIN numbers may be required to be 7 digits;
d) Voice mail PIN numbers may not be easily guessed from the telephone number of the mailbox.

5.2.4 Timing of Authentication (FIA_UAU.2)

5.2.4.1 FIA_UAU.2.1. The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on be behalf of that user.

5.2.5 Protected authentication feedback (FIA_UAU.7)

5.2.5.1 FIA_UAU.7.1 The TSF shall provide only [assignment: *no feedback, minimal feedback, or the following*

- *The TSF shall not transmit a response to any part of the login sequence until the entire login sequence has been completed.*
- *Upon successful login, the TSF shall display the date and time of the last successful login by the user and the number of unsuccessful attempts (if any) since the last login.*
- *If the switch has DISA deployed, the PBX will not provide any helpful suggestions until both the DISA-DN and DISA-PIN are correctly and sequentially provided.*]

to the user while the authentication is in progress.

5.2.6 User Identification Before Any Action

5.2.6.1 FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.2.7 User-Subject Binding (FIA_USB.1)

5.2.7.1 FIA_USB.1.1. The TSF shall associate the appropriate user security attributes with subjects acting on the behalf of that user:

5.3 TOE Access (FTA)

5.3.1 Limitation on scope of selectable attributes (FTA_LSA.1)

5.3.1.1 FTA_LSA.1.1. FTA_LSA.1.1. The TSF shall restrict the scope of the session security attributes [assignment: *access permissions, audit requirements, other session security attributes*] based on [assignment: *session type, ports, network identification of the specific requestor, date and time, other attributes*].

For example, if an *output* port receives a login request, the PBX shall not respond. The PBX shall have the capability to restrict a login based upon the date, time, and network identification of the specific requestor.

5.3.2 TSF-initiated session locking (FTA_SSL.1)

5.3.2.1 FTA_SSL.1.1. The TSF shall lock an interactive session after [assignment: *time interval of user inactivity*] by:

a) Clearing or overwriting display devices, making the current contents unreadable;
b) Disabling any activity of the user's data access/display devices other than unlocking the session.
c) Locking the channel for subsequent *inputs*, other than re-authentication actions, although the TSF shall be able to transmit over the locked channel.

5.3.2.2 FTA_SSL.1.2. The TSF shall require the following events to occur prior to unlocking the session:

a) Re-authentication of the user
b) [assignment: *Other events as specified by the ST*].

Application Note: Sessions established by other network components that are identified and authenticated as "users" are not considered interactive sessions. The TSF shall have the capability of distinguishing between these two types of sessions. The TSF may then disable the time-out feature for network component sessions even if they stay logged on to the PBX for extended periods of time.

5.3.3 User-initiated session locking (FTA_SSL.2)

5.3.3.1 FTA_SSL.2.1. The TSF shall allow user-initiated locking of the user’s own interactive session, by:

a) clearing or overwriting display devices, making the current contents unreadable;
b) disabling any activity of the user’s keyboard or other data access/display devices other than unlocking the session.

5.3.3.2 FTA_SSL.2.2. The TSF shall require the following events to occur prior to unlocking the session:

a) re-authentication of the used,
b) [assignment: *Other events as specified by an authorized administrator*].

5.3.4 TSF-initiated termination (FTA_SSL.3)

5.3.4.1 FTA_SSL.3.1. The TSF shall terminate an interactive session after a [assignment: *time interval of user inactivity, power failure, link disconnection*].

5.3.5 Default TOE access banners(FTA_TAB.1)

5.3.5.1 FTA_TAB.1.1. At the time of login, the TSF shall generate a warning banner. The message transmitted in the banner shall be specifiable by an authorized administrator to meet local requirements and state laws.

5.3.6 TOE access history (FTA_TAH.1)

5.3.6.1 FTA_TAH.1.1. Upon successful login, the TSF shall display the [selection: *date, time, method, location*] of the last successful login, the number of unsuccessful attempts (if any) since the last login, and the date and time of the last unsuccessful attempt.

5.3.6.2 FTA_TAH.1.3. The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

5.3.7 TOE Session establishment (FTA_TSE.1)

5.3.7.1 FTA_TSE.1.1. The TSF shall be able to deny session establishment based on [assignment:

- *When a session is terminated (i.e., when a logoff occurs), the port shall drop immediately so that a subsequent user has to re-authenticate to initiate the next session.*
- *Before allowing a session (i.e., a login), the TSF shall require a session requester to provide the identifier as well as the authenticator. All access ports, except the Emergency Access Interface*[4] *(EAI) shall be equipped with this login feature.*
- *If unauthenticated access is provided over a Data Communications Channel (DCC), as in the case of a Synchronous Optical Network (SONET), the TSF shall control access, if necessary by using a peripheral device such as a firewall.*
- *If the PBX is equipped with an EAI, the EAI shall have the following features to provide protection against intrusion: The TOE shall activate an alarm when the EAI is in operation. The TSF shall prevent the EAI from accepting any commands other than those considered essential for performing system restoration.*]

4 A PBX may be equipped with an EAI which allows a session without requiring a login so that in the case of an emergency, when the regular login feature does not function, the PBX, as a minimum, can be restored via the EAI. There are ways to protect the EAI against intrusion, as described in the next requirement.

Application Notes:

1. All software changes shall be documented and reviewed to ascertain that security has not been compromised.
2. At the time of delivery and installation, the PBX shall be provided with secure installation defaults.
3. An administrator shall have the capability to customize the default security parameters (e.g., default user identifiers, default authenticators, default settings for access permission levels for various system resources, etc.) at any time during the installation process.
4. There shall be test procedures to determine whether the delivered software is exactly as specified in the master copy.

5.4 Cryptographic Support (FCS)

5.4.1 Cryptographic Operation (FCS_COP.1)

This section is relevant only for applications where several distributed PBX systems and their admin facilities are interconnected via networks.[5] The PP requirements described in this section are not applicable to a stand-alone PBX and its adjuncts.

5.4.1.1 FCS_COP.1.1.

The TSF shall support the Telecommunications Management Network (TMN) based switch management system specified by the International Telecommunication Union (ITU) to provide protection for transactions between PBXs and the integrity of the Common Management Information Protocol (CMIP) based messages that are exchanged between a PBX and an Admin facility. To provide this functionality, the TSF shall either support the "Security Transformations Application Service Element for Remote Operations Service Element" (STASE-ROSE) as described in Section 5.4.1.2 or the alternative specified in Section 5.4.1.3.

The TSF shall support the default public key authenticator defined in the standard T1.259, along with exchange of a symmetric session key.

5.4.1.2 STASE-ROSE

STASE-ROSE shall support the following security transformations (ST)s[6]:

- **confidential:** The DER-encoded ROSE PDU shall be encrypted for privacy protection with a symmetric key encryption algorithm.
- **hashed:** a hash-based Message Authentication Code (MAC) of the DER-encoded ROSE PDU and a secret password shall be calculated and the results appended to the ROSE PDU for integrity protection.
- **confidential hashed:** The MAC of the DER-encoded ROSE PDU shall be computed and the results appended to the encrypted (see "confidential" above) ROSE PDU for integrity and privacy protection.

5.4.1.3 STASE-ROSE Alternative for TCP/IP

If all network management transactions are transported over TCP/IP, it is not required for the TSF to support STASE-ROSE. If STASE-ROSE is not provided by the TSF for TCP/IP transactions, the TSF shall use the Secure Socket Layer version 3 (SSL3). The TSF implementation of SSL3 shall support the following:

---

5 Centralized administrative facilities may include administration of applications related to Computer Telephony Integration (CTI), Distributed Call Centers, Help Desk, PC Fax, Desktop Video, Website Interactive Voice Response (IVR), etc.

6 STASE-ROSE protects ROSE PDUs by applying selected security transformations (ST) to whole ROSE PDUs encoded with the Distinguished Encoding Rules (DER).

- Strong peer entity authentication, based on public key encryption shall be provided for all associations (this precludes interoperability with SSL2)
- Session secret shall be encrypted with receiver's public key
- SHA1 shall be used for integrity by SSL3
- If privacy protection by SSL3 is provided, then DES (Data Encryption Standard) in the CBC (Cipher Block Chaining) mode shall be used for symmetric key encryption
- A public key certificate from the TMN's CA is required
- Integrity and non-repudiation shall be computed on clear text (unencrypted) messages,
- Entity public key size shall be at least 768 bits
- CA's public key size shall be at least 1024 bits
- Certificates shall be X.509 version 3.
- The following ciphersuites will be supported:
  - RSA, NULL, SHA1 (if no privacy protection is desired)
  - RSA, DES - CBC, SHA1 (if privacy protection is desired)

5.5 User Data Protection (FDP)

5.5.1 Complete Access Control (FDP_ACC.2)

5.5.1.1 FDP_ACC.2.1 The TSF shall enforce the PBX Access Control Policy on all subjects and objects and all operations among subjects and objects covered by the TSP.

5.5.1.2 FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control mechanism as described in the TSP.

5.5.2 Access Control Functions (FDP_ACF.1)

5.5.2.1 FDP_ACF.1.1. The TSF shall enforce the Access Control Policy to objects based on [assignment:

a) *The user identity and group membership(s) associated with a subject; and*
b) *The access control attributes and permissions associated with an object.*]

5.5.2.2 FDP_ACF.1.2. The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment:

a) *Rule(s) defined by an authorized administrator which use the user identity of a subject as the basis of allowing or denying access, including limiting the propagation of access rights to objects;*
b) *Rule(s) defined by an authorized administrator which are used to allow or deny access when user identity rules do not apply, such as those based upon time of day, port, or location.*]

5.5.2.3 FDP_ACF.1.3. The TSF shall explicitly authorize access of subjects to objects based on the following additional rules:

a) After the PBX receives a correct sequence of DISADN and DISA-PIN, the PBX shall provide a second dial tone but shall allow only the call processing service that has been authorized for that subscriber,
b) [assignment: *other rules, based on security attributes, that explicitly authorize access of subjects to objects*].

5.5.2.4 FDP_ACF.1.4. The TSF shall explicitly deny access of subjects to objects based on the following rules [assignment:

a) *The PBX System*[7] *shall not allow resource access to any user who has not established system access (i.e., a login with identification and authentication).*
b) *Unless a user has permission to access a resource, the PBX System shall deny the access.*
c) *Unless a port has permission to access a resource, the PBX shall deny the access to all users who log into that port.*

[7] The PBX System includes the PBX and its adjuncts (e.g., voice mail and automated attendant).

d) *The level of granularity of the resource control mechanism shall be such that, any given user that has logged into any given port can be granted access or denied access to any given resource (based on the user privilege and the port privilege).*
e) *The PBX System shall have the capability to lock away potentially damaging commands (e.g., delete all translations) from users who do not need to execute such commands on a "regular basis" and from ports that are not intended to be used for such commands.*
f) *The PBX System shall have the capability to impose access control on the basis of functions such as Create, Read, Update, and Delete (CRUD).*
g) *The PBX System shall not offer any mechanism to bypass authorization restrictions.*
h) *The PBX System shall not allow a less privileged user to spoof as a highly privileged user (such as a Superuser in a UNIX environment).*
i) *The PBX System shall have features to assign user privileges (i.e., access permissions) to user-IDs (not passwords8).*
j) *For PBX Systems that have multiple operations ports, the System shall have features to assign privileges to input ports.*
k) *For PBX subscribers, the PBX shall have adequate granularity for "call restriction" (e.g., other extensions only, local calls only, intra-LATA toll calls, long distance calls, international calls, etc.)*
l) *For DISA deployed systems, the PBX shall not allow any DISA subscriber to establish direct access to a trunk unless the subscriber first provides the correct DISADN/PIN combination (i.e. there shall be no bypass mechanism).*
m) *The Voice Mail system will not provide a second dial tone to an outside user after providing a message.*
n) *If an automated attendant is connected to a PBX, the attendant shall have the capability to deny a second dial tone to an outside caller.*]

5.5.3 Residual Information Protection (FDP_RIP.2)

5.5.3.1 FIP_RIP.2.1. The TSF shall ensure that any previous information content of a resource is made unavailable upon the re-allocation of the resource to any object - except for references contained in the audit trail.

8 Assigning user privileges to passwords may compromise their confidentiality.

5.6 Class FAU: Security Audit

5.6.1 Security Alarms (FAU_ARP.1)

- FAU_ARP.1.1. The TSF shall take [assignment: *list of the least disruptive actions*] upon detection of a potential security violation.

5.6.2 Audit Data Generation (FAU_GEN.1)

5.6.2.1 FAU_GEN.1.1. The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- All auditable events for the [*basic*] level of audit, including:
  - Modifications of security attributes;
  - Attempts to revoke security-relevant authorizations;
  - Attempts to revoke access rights;
  - Changes to the time;
- [assignment: *Other specifically defined auditable events:*
  - *Changes to system software that is part of the TOE that lies outside the TSF. Modification to the TSF is not allowed, once evaluated; however modification to other essential software (e.g. billing) that does not affect the security policy may be modified.*]

5.6.2.2 FAU_GEN 1.2. The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure[9]) of the event.

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST [assignment:
   - *For Identification and Authentication events, the origin (e.g., terminal identification) of the attempt.*
   - *For modifications to TSF data, the new values of the data.*
   - *For the use of the rights of a role[10], when it could originate from multiple locations, the origin of the attempt.*
   - *Other audit relevant information identified in the ST*:]

9 Application Note: Failures need not record a discrete event in the audit log. Failures may be recorded as the collection of several positive events.

10 Application Note: For example, administrators may logon to the console or an alternate location.

5.6.3 User Identity Association (FAU_GEN.2)

5.6.3.1 FAU_GEN.2.1. The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Application Note: the audit requirements therefore must include:

- For each event recorded in the security log, the PBX shall also record the identifier of the user (the user-ID) that is accountable for the event.
- For software and data created or modified in the PBX, the PBX shall provide an administrator the capability to retrieve the user-ID, date and time associated with that creation or modification.

5.6.4 Potential violation analysis (FAU_SAA.1)

5.6.4.1 FAU_SAA.1.1. The TSF shall apply a set of rules in monitoring the audited events and base these rules upon potential violations of the TSP.

5.6.4.2 FAU_SAA.1.2. The TSF shall enforce the following rules for monitoring audited events:

- Accumulation or combination of [assignment:
  - *logon failures to system software, DISA, or voice-mail system;*
  - *other rules as identified in the Security Target*].
- [assignment: *any other rules*].

5.6.5 Audit Review (FAU_SAR.1)

5.6.5.1 **FAU_SAR.1.1**. The TSF shall provide authorized administrators with the capability to read [assignment:

a) *Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event.*
b) *For applicable events, the names of the resources accessed.*
c) *For Identification and Authentication events, the origin (e.g., terminal identification) of the attempt.*
d) *For modifications to TSF data, the new values of the data.*
e) *For the use of the rights of a role, when it could originate from multiple locations, the origin of the attempt.*
f) *Other audit relevant information.*]

from the audit records.

5.6.5.2 **FAU_SAR.1.2**. The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.6.6 Restricted Audit Review (FAU_SAR.2)

5.6.6.1 **FAU_SAR.2.1.** The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.6.7 Guarantees of Audit Data Availability (FAU_STG.2)

5.6.7.1 **FAU_STG.2.1**. The TSF shall protect the stored audit records from unauthorized deletion.

5.6.7.2 **FAU_STG.2.2.** The TSF shall be able to detect modifications to the audit records.

5.6.7.3 **FAU_STG.2.3.** The TSF shall ensure that the capacity of the audit file is sufficient to store at least 24 hours of audit records even when the following conditions occur: audit storage exhaustion.

5.6.8 Action in case of possible audit data loss (FAU_STG.3)

5.6.8.1 **FAU_STG.3.1.** The TSF shall send an alarm to the authorized administrator if the audit trail exceeds an authorized administrator defined limit.

5.6.9 Prevention of Audit Data Loss (FAU_STG.4)

5.6.9.1 **FAU_STG.4.1.** The TSF shall overwrite the oldest stored audit records if the audit trail is full.

5.7 Security Management (FMT)

5.7.1 Management of Security Functions (FMT_MOF.1)

5.7.1.1 FMT_MOF.1.1. The TSF shall restrict the ability to:

- *determine the behavior of,*
- *enable,*
- *disable, and*
- *modify the behavior of*

the functions [assignment:

- *Audit,*
- *Password Management,*
- *Roles,*
- *Users management, and*
- *other functions*]

to [assignment: *authorized administrators, other authorized identified roles*]

5.7.2 Management of Object Security Attributes (FMT_MSA.1)

5.7.2.1 FMT_MSA.1.1. The TSF shall enforce the *Access Control Policy* to restrict the ability to *modify* the security attributes: [assignment: *userid, password, roles, or other security attributes associated with a named object*] to *the authorized identified roles.*

5.7.3 Management of the Security Data (FMT_MTD.1)

5.7.3.1 FMT_MSA.1.1. The TSF shall enforce the *Access Control Policy* to restrict the ability to *modify* the security attributes: [assignment: *userid, password, roles, or other security attributes associated with a named object*] to *the authorized identified roles.*

5.7.4 Security attribute expiration (FMT_SAE)

5.7.4.1 FMT_SAE.1.1. The TSF shall restrict the capability to specify an expiration time for: *DISA-PIN numbers (if DISA is deployed), Voice Mailbox PIN numbers, and user passwords* to *authorized administrators.*

5.7.4.2 FMT_SAE.1.2. For each of these security attributes, the TSF shall be able to:

a) require the user to select a new value for the attribute, or
b) require the authorized system administrator to assign a new value to the attribute, or

c) generate an alarm and suspend all user access until reactivated by the authorized system administrator

after the expiration time for the indicated security attribute has passed.

6 Assurance Requirements

This chapter defines the assurance requirements for the TOE from Part 3 of the CC.

6.1 Configuration Management (ACM)

6.1.1 Authorization Controls (ACM_CAP.3)

6.1.1.1 ACM_CAP.3.1D. The developer shall provide a reference for the TOE.

6.1.1.2 ACM_CAP.3.2D. The developer shall use a CM system. The developer shall demonstrate that the identified CM system is employed for all TSF development.

6.1.1.3 ACM_CAP.3.3D. The developer shall provide CM documentation that describes the CM system including the implementation and how the CM system has been used to control the development of the TSF.

6.1.1.4 ACM_CAP.3.1C. The reference for the TOE shall be unique to each version of the TOE.

6.1.1.5 ACM_CAP.3.2C. The TOE shall be labeled with its reference.

6.1.1.6 ACM_CAP.3.3C. The CM documentation shall include a configuration list and a CM plan.

6.1.1.7 ACM_CAP.3.4C. The configuration list shall describe the configuration items that comprise the TOE.

6.1.1.8 ACM_CAP.3.5C. The CM documentation shall describe the method used to uniquely identify the configuration items.

6.1.1.9 ACM_CAP.3.6C. The CM system shall uniquely identify all configuration items.

6.1.1.10 ACM_CAP.3.7C. The CM plan shall describe how the CM system is used.

6.1.1.11 ACM_CAP.3.8C. The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

6.1.1.12 ACM_CAP.3.9C. The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

6.1.1.13 ACM_CAP.3.10C. The CM system shall provide measures such that only authorized changes are made to the configuration items.

6.1.1.14 ACM_CAP.3.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application Note: This component provides for three things. First it requires that the TOE being identifiable by a customer, using things such as version and part numbers, to ensure that the proper thing has been installed. Second it requires that the materials used to produce the TOE, such as source code and design documentation be identified. And third it requires that the production of the TOE be done in a controlled manner.

6.1.2 Coverage (ACM_SCP.1)

6.1.2.1 ACM_SCP.1.1D. The developer shall provide CM documentation.

6.1.2.2 ACM_SCP.1.1C. The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation.

6.1.2.3 ACM_SCP.1.2C. The CM documentation shall describe how configuration items are tracked by the CM system.

6.1.2.4 ACM_SCP.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2 Delivery and Operation (ADO)

6.2.1 Delivery Procedures (ADO_DEL.1)

6.2.1.1 ADO_DEL.1.1D. The developer shall document procedures for delivery of the TOE or parts of it to the user.

6.2.1.2 ADO_DEL.1.2D. The developer shall use the delivery procedures.

6.2.1.3 ADO_DEL.1.1C. The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

6.2.1.4 ADO_DEL.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application Note: The delivery procedures for a CAPP conformant TOE can vary greatly and can range from a shrink wrapped box from a retail outlet to delivery by a field engineer. As such, there may be opportunities for third parties to tamper with the TOE delivery process. In these cases the developer should provide procedures or mechanisms to mitigate the threat.

6.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

6.2.2.1 ADO_IGS.1.1D. The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

6.2.2.2 ADO_IGS.1.1C. The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

6.2.2.3 ADO_IGS.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.2.4 ADO_IGS.1.1E. The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

Application Note: The required documentation depends on the way in which a TOE is generated and installed. For example the generation of a TOE from source code may be done at the development site, in which case the required documentation would be considered part of the design documentation. On the other hand, if some part of the TOE generation is done by the TOE administrator, it would be part of the administrative guidance. Similar circumstances could also apply to both installation and start-up procedures.

6.3 Development (ADV)

6.3.1 Functional Specification (ADV_FSP.1)

6.3.1.1 ADV_FSP.1.1D. The developer shall provide a functional specification.

6.3.1.2 ADV_FSP.1.1C. The functional specification shall describe the TSF and its external interfaces using an informal style.

6.3.1.3 ADV_FSP.1.2C. The functional specification shall be internally consistent.

6.3.1.4 ADV_FSP.1.3C. The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

6.3.1.5 ADV_FSP.1.4C. The functional specification shall completely represent the TSF.

6.3.1.6 ADV_FSP.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.1.7 ADV_FSP.1.2F. The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

Application Note: This components requires that the design documentation includes a complete description of the TSF as seen from outside it. In particular it needs to address the

mechanisms which are used to meet the functional requirements of the PP. Other areas need to be addressed to the degree that they impact upon the functional requirements.

6.3.2 High-Level Design (ADV_HLD.2)

6.3.2.1 ADV_HLD.2.1D. The developer shall provide the high-level design of the TSF.

6.3.2.2 ADV_HLD.2.1C. The presentation of the high-level design shall be informal.

6.3.2.3 ADV_HLD.2.2C. The high-level design shall be internally consistent.

6.3.2.4 ADV_HLD.2.3C. The high-level design shall describe the structure of the TSF in terms of subsystems.

6.3.2.5 ADV_HLD.2.4C. The high-level design shall describe the security functionality provided by each subsystem of the TSF.

6.3.2.6 ADV_HLD.2.5C. The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

6.3.2.7 ADV_HLD.2.6C. The high-level design shall identify all interfaces to the subsystems of the TSF.

6.3.2.8 ADV_HLD.2.7C. The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

6.3.2.9 ADV_HLD.2.8C. The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

6.3.2.10 ADV_HLD.2.9C. The high-level design shall describe the separation of the TSF into TSP-enforcing and other subsystems.

6.3.2.11 ADV_HLD.2.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.2.12 ADV_HLD.2.2E. The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

Application Note: This component requires that the design documentation include a breakdown of the TSF at a very coarse grain. Both the developer and evaluator need to carefully chose how a "subsystem" is defined for a particular TOE. There must be a balance between subsystems being too large that it is difficult to understand the functions of any

single subsystem and subsystems that are so small that how they fit into the system as a whole is difficult to understand. If different pieces of the TSF are developed or maintained by different groups of developers, that can serve in making those choices.

Furthermore, it must be noted that the presentation need only be informal. This means that the interfaces between subsystems need to be presented to general terms of how they interact, not to the level of presenting an API between them.

6.3.3 Correspondence Demonstration (ADV_RCR.1)

6.3.3.1 ADV_RCR.1.1D. The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

6.3.3.2 ADV_RCR.1.1C. For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

6.3.3.3 ADV_RCR.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application Note: For this PP, this apply to ensure that the functional specification and high-level design are consistent with each other.

6.4 Guidance Documents (AGD)

6.4.1 Administrator Guidance (AGD_ADM.1)

6.4.1.1 AGD_ADM.1.1D. The developer shall provide administrator guidance addressed to system administrative personnel.

6.4.1.2 AGD_ADM.1.1C. The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

6.4.1.3 AGD_ADM.1.2C. The administrator guidance shall describe how to administer the TOE in a secure manner.

6.4.1.4 AGD_ADM.1.3C. The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

6.4.1.5 AGD_ADM.1.4C. The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

6.4.1.6 AGD_ADM.1.5C. The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

6.4.1.7 AGD_ADM.1.6C. The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

6.4.1.8 AGD_ADM.1.7C. The administrator guidance shall be consistent with all other documents supplied for evaluation.

6.4.1.9 AGD_ADM.1.8C. The administrator guidance shall describe all security requirements on the IT environment that are relevant to the administrator.

6.4.1.10 AGD_ADM.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application Note: The content required by this component is quite comprehensive and broadly stated; in particular the content needs to address any of the mechanisms and functions provided to administrator to meet the functional requirements of this PP. It should also contain warnings about certain actions that, may typically be done by administrators, which should not be done with the TOE. This could include turning on certain functions or installing certain software which would compromise the TSF.

6.4.2 User Guidance (AGD_USR.1)

6.4.2.1 AGD_USR.1.1D. The developer shall provide user guidance.

6.4.2.2 AGD_USR.1.1C. The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

6.4.2.3 AGD_USR.1.2C. The user guidance shall describe the use of user-accessible security functions provided by the TOE.

6.4.2.4 AGD_USR.1.3C. The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

6.4.2.5 AGD_USR.1.4C. The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

6.4.2.6 AGD_USR.1.5C. The user guidance shall be consistent with all other documentation supplied for evaluation.

6.4.2.7 AGD_USR.1.6C. The user guidance shall describe all security requirements on the IT environment that are relevant to the user.

6.4.2.8 AGD_USR.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application Note: The content required by this component is quite comprehensive and broadly stated; in particular the content needs to address any of the mechanisms and functions provided to user to meet the functional requirements of this PP. It should also contain warnings about certain actions, that are typically done by users, which should not be done with the TOE.

6.5 Life Cycle Support (ALC)

6.5.1 Identification of Security Measures (ALC_DVS.1)

6.5.1.1 ALC_DVS.1.1D. The developer shall produce development security documentation.

6.5.1.2 ALC_DVS.1.1C. The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

6.5.1.3 ALC_DVS.1.2C. The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

6.5.1.4 ALC_DVS.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.5.1.5 ALC_DVS.1.2E. The evaluator shall confirm that the security measures are being applied.

Application Note: For this PP, this is really an extension of configuration management system requirements to ensure that TSF is subverted by outsiders during development.

6.6 Security Testing (ATE)

6.6.1 Coverage (ATE_COV.2)

6.6.1.1 ATE_COV.2.1D. The developer shall provide an analysis of the test coverage.

6.6.1.2 ATE_COV.2.1C. The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

6.6.1.3 ATE_COV.2.2C. The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

6.6.1.4 ATE_COV.2.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.6.2 Depth (ATE_DPT.1)

6.6.2.1 ATE_DPT.1.1D. The developer shall provide the analysis of the depth of testing.

6.6.2.2 ATE_DPT.1.1C. The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

6.6.2.3 ATE_DPT.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application Note: While the high-level design is to be used as the basis for testing, it is not required that internal interfaces between subsystems be tested.

6.6.3 Functional testing (ATE_FUN.1)

6.6.3.1 ATE_FUN.1.1D. The developer shall test the TSF and document the results.

6.6.3.2 ATE_FUN.1.2D. The developer shall provide test documentation.

6.6.3.3 ATE_FUN.1.1C. The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

6.6.3.4 ATE_FUN.1.2C. The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

6.6.3.5 ATE_FUN.1.3C. The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

6.6.3.6 ATE_FUN.1.4C. The expected test results shall show the anticipated outputs from a successful execution of the tests.

6.6.3.7 ATE_FUN.1.5C. The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

6.6.3.8 ATE_FUN.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.6.4 Independent Testing (ATE_IND.2)

6.6.4.1 ATE_IND.2.1D. The developer shall provide the TOE for testing.

6.6.4.2 ATE_IND.2.1C. The TOE shall be suitable for testing.

6.6.4.3 ATE_IND.2.2C. The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

6.6.4.4 ATE_IND.2.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.6.4.5 ATE_IND.2.2E. The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

6.6.4.6 ATE_IND.2.3E. The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

Application Note: The choice of the subset tested and sample of tests executed by the evaluator is entirely at the discretion of the evaluator.

6.7 Vulnerability Assessment (AVA)

6.7.1 Examination of Guidance (AVA_MSU.1)

6.7.1.1 AVA_MSU.1.1D. The developer shall provide guidance documentation.

6.7.1.2 AVA_MSU.1.1C. The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

6.7.1.3 AVA_MSU.1.2C. The guidance documentation shall be complete, clear, consistent and reasonable.

6.7.1.4 AVA_MSU.1.3C. The guidance documentation shall list all assumptions about the intended environment.

6.7.1.5 AVA_MSU.1.4C. The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

6.7.1.6 AVA_MSU.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.7.1.7 AVA_MSU.1.2E. The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

6.7.1.8 AVA_MSU.1.3. The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

Application Note: This requirement is can be approached as testing by the evaluator to ensure that the guidance documents are correct. The content elements primarily reinforce the guidance requirements themselves.

6.7.2 Strength of TOE Security Function Evaluation (AVA_SOF.1)

6.7.2.1 AVA_SOF.1.1D. The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

6.7.2.2 AVA_SOF.1.1C. For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

6.7.2.3 AVA_SOF.1.2C. For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

6.7.2.4 AVA_SOF.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.7.2.5 AVA_SOF.1.2E. The evaluator shall confirm that the strength claims are correct.

Application Note: For the CAPP, the requirement applies to the authentication mechanism which is used as described in 5.2.3.

6.7.3 Developer Vulnerability Analysis (AVA_VLA.1)

6.7.3.1 AVA_VLA.1.1D. The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

6.7.3.2 AVA_VLA.1.2D. The developer shall document the disposition of obvious vulnerabilities

6.7.3.3 AVA_VLA.1.1C. The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

6.7.3.4 AVA_VLA.1.1E. The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.7.3.5 AVA_VLA.1.2E. The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

Application Note: The evaluator should consider the following with respect to the search for obvious flaws:

a) Dependencies among functional components and potential inconsistencies in strength of

function among interdependent functions;

b) Potential inconsistencies between the TSP and the functional specification;

c) Potential gaps or inconsistencies in the HLD, and potentially invalid assumptions about supporting hardware, firmware, and/or software required by the TSF;

d) Potential gaps in the administrator guidance that enable the administrator to fail (a) to make effective use of TSF functions, (b) to understand or take actions that need to be performed, (c) to avoid unintended interactions among security functions, and (d) to install and/or configure the TOE correctly. In particular, failure to describe all the security parameters under the administrator's control and the effects of settings of (interacting combinations of) those parameters;

e) Potential gaps in the user guidance that enable the user to fail to control functions and privileges as required to maintain a secure processing environment. Potential presence in the user guidance of information that facilitates exploitation of vulnerabilities;

f) Open literature (e.g., CERT advisories, bug-traq mailing list) which may contain information on vulnerabilities on the TSF and these sources should be consulted.

7 Rationale

7.1 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, security objective, and component that comprise the protection profile.

7.1.1 Complete Coverage – Threats, Organizational Security Policies, and Security Usage Assumptions

This section provides evidence demonstrating coverage of the threats, organizational security policies, and security usage assumptions by both IT and non-IT security objectives. Table 7.1.1.1 illustrates this coverage.

Table 7.1.1.1. Traceability of Security Objectives

Security Objectives	Threats	Organizational Security Policies	Security Usage Assumptions
IT Security Objectives			
O.KNOWN: The TOE shall ensure that, except for a well-defined set of allowed actions, all users are identified and authenticated before being granted access.	Insecure Security System	P.Access P.Confidentiality	A.Cearance A.Physical Authorization
O.ACCESS: The TOE shall allow access by authenticated users to those TOE resources for which they have been authorized, and deny access to those TOE resources for which they are not authorized.	Access Misuse; Insecure Security System; Fraud	P.Access P.Confidentiality	A.Clearance
O.AUTHORIZE: The TOE shall provide the ability to specify and manage “resource access permission” to be assigned to its users.	Access Misuse;	P.Administration	A.Clearance
O.BYPASS: The TOE shall prevent all software and users from bypassing or circumventing TOE security policy enforcement.	Access Misuse; Intrusion; Insecure Security System	P.Access	A.Training A.Clearance
O.MISUSE: The TOE shall mitigate the threat of malicious actions by authenticated users	Fraud Access Misuse;	P.TMN P.Traceability P.Accountability P.Usage	A.Regress A.Audit A.Clearance
O.ACCOUNT: The TOE shall ensure that all TOE users can be held	Insecure Security System;	P.Accountability P.Usage	A.Regress A.Audit

Security Objectives	Threats	Organizational Security Policies	Security Usage Assumptions
accountable for their security-relevant actions.	Access Misuse; Intrusion		
O.INFO-FLOW: The TOE shall ensure that any information flow control policies are enforced – (1) between TOE components and (2) at the TOE external interfaces.	Intrusion; Access Misuse	P.Confidentiality	A.InsecureRemote A.Insecure Network
O.OBSERVE: The TOE shall ensure that its security status is not misrepresented to the administrator or user.	Insecure State Transition; Insecure Security System	P.Traceability	
O.DETECT: The TOE shall have the capability to detect system failure and breech of security.	Insecure Security System; Fraud	P.Traceability	A.Expertise
O.RECOVER: The TOE shall provide for recovery to a secure state following a system failure, discontinuity of service, or detection of a security flaw or breech.	Insecure State Transition;	P.Availability P.Resiliency	A.Expertise
O.AVAILABLE: The TOE shall protect itself from denial-of-service attacks, including shared resource exhaustion.	Denial of Service	P.Availability P.Resiliency	A.Natural A.Environment A.Hardware
O.NETWORK: Unless explicitly stand-alone, the TOE shall have the capability to meet its security objectives in a distributed environment.	Physical Threat; Access Misuse	P.TMN	A.InsecureRemote A.Insecure Network A.Protocols A.Ingress
O.CONFIDENTIAL: The TOE shall have the ability to identify confidential information. Such information may be related to customers, subscribers, or system security. The TOE shall release confidential information only to authorized users.	Access Misuse; Intrusion;	P.Confidentiality P.TMN	A.Clearance
Non-IT Security Objectives			

Security Objectives	Threats	Organizational Security Policies	Security Usage Assumptions
O.PHYSICAL: An administrator responsible for TOE security shall ensure that the TOE environment has adequate physical security to provide "reasonable safety" (as described earlier) to TOE resources.	Physical Threat	P.Administration	A.Environment
O.OPERATE: An administrator responsible for TOE security shall ensure that the TOE is delivered, installed, and operated in a manner which maintains IT security.	Insecure Security System	P.Administration	A.Expertise A.Training
O.MANAGE: An administrator responsible for TOE security shall ensure that the TOE is managed and administered in a manner that maintains IT security.	Insecure Security System	P.Administration	A.Audit A.Expertise
O.COMPLY: The TOE environment shall support full compliance with laws, regulations, and contractual agreements.	Access Misuse;	P.TMN	A.Hardware

7.2 Security Requirements Rationale

This section provides evidence supporting the combined internal consistency and completeness of the functional and security requirements that comprise the PBXPP.

Table 7.2-1 demonstrates that the functional components and assurance requirements selected for this profile provide complete coverage of the defined security objectives.

Table 7.2-1. Coverage of Security Objectives

Security Requirements	**SECURITY OBJECTIVES**
Functional Requirements	
5.1 Security Audit (FAU)	O.ACCOUNT
5.1 User Data Protection (FDP)	O.ACCESS O.BYPASS O.MISUSE O.RECOVER O.AVAILABLE O.EQUAL-ACCESS O.PHYSICAL O.DENIAL O.COMPLY
5.2 Identification and Authentication (FIA)	O.KNOWN O.ENTRY O.AUTHORIZE

	O.NETWORK
5.3 Security Management (FMT)	O.MANAGE O.OBSERVE O.DETECT O.RECOVER
5.4 Protection of the TOE Security Functions (FPT)	O.BYPASS O.INFO-FLOW
Assurance Requirements	
6.1 Configuration Management (ACM)	O.OPERATE O.MANAGE
6.2 Delivery and Operation (ADO)	O.OPERATE O.RESILIENCY
6.3 Development (ADV)	O.OPERATE
6.4 Guidance Documents (AGD)	O.MANAGE O.COMPLY
6.5 Life Cycle Support (ALC)	O.OPERATE O.MANAGE
6.6 Security Testing (ATE)	O.OPERATE
6.7 Vulnerability Assessment (AVA)	O.MANAGE

7.2.1 Internal Consistency of Requirements

This section describes the mutual support and internal consistency of the components selected for this profile. These properties are discussed for both functional and assurance components.

The functional components were selected from pre-defined CC components. The use of component refinement was accomplished in accordance with CC guidelines. An additional component was included to clarify the relationship of objects and security attributes.

Assignment, selection, and refinement operations were carried out among components using consistent computer security terminology. This helps to avoid the ambiguity associated with interpretations of meanings of terms between related components.

Multiple instantiation of identical or hierarchically related components was used to clearly state the required functionality that must exist in a TOE conformant with this profile.

8 Acronym List

CC	-	Common Criteria.
CCS	-	Common Channel Signaling network.
CMIP	-	Common Management Information Protocol.
DES	-	Digital Encryption Standard
DES3	-	Triple DES
DISA	-	Direct Inward System Access
ESP	-	Encapsulated Security Payload
HMAC	-	Hash Message Authentication Code
IKE	-	Internet Key Exchange protocol
PBX	-	Private Branch Exchange
PBXPP	-	PBX Switch Protection Profile
PP	-	Protection Profile.
SHA1	-	Secure Hash Algorithm, version 1
ST	-	Security Target.
TMN	-	Telecommunications Management network.
TOE	-	Target of Evaluation.
TSF	-	TOE Security Function.
TSP	-	TOE Security Policy.